UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

* * *

UNITED STATES OF AMERICA, Plaintiff, v. CHARLES A. BOROWY, Defendant.	3:08-CR-00007-LRH-VPC ORDER

Before the court is Defendant Charles A. Borowy's Motion to Suppress Evidence (#20[1]). The Government has responded (#23).

I. Facts[2]

On May 3, 2007, Special Agent Byron Mitchell of the FBI, operating undercover, logged into a peer to peer (P2P) file-sharing program called Limewire to monitor the trafficking of child pornography. P2P file sharing is a means of sharing files directly between computers without resort to a centralized server to route or store the files. In P2P file sharing, a network of computers is usually linked over the internet using special software installed on all computers in the network. A user can open this software at his computer and conduct a keyword search for files that are currently

[1]Refers to court's docket number

[2]The facts are taken from Special Agent Jeff Cotner's affidavit in support of a search warrant unless otherwise noted. (Mot. to Suppress (#20), Cotner Aff., Ex. A ¶¶ 25-38.)

being shared on the network. The search returns a list of files along with the Internet Protocol (IP) addresses of the computers on which the files are stored.[3] The user can select certain files from the displayed results and download them directly onto his computer from the computer on which the files are stored.

On May 3, 2007, Agent Mitchell conducted a search in Limewire using the term "Lolitaguy," which is known to be associated with images of child pornography. In response to his search, a list of results appeared, including one file located at a specific IP address. After connecting to this IP address, Agent Mitchell obtained a list of files that the address user was currently sharing. Several filenames on the list were consistent with filenames for child pornography files.

Agent Mitchell initiated several downloads from the approximately 240 files listed. After completing seven downloads, Agent Mitchell viewed and recorded the downloads' content. All of the downloaded files were videos, and four of these videos appeared to be child pornography.

Agent Mitchell confirmed through his download logs the specific IP address from which all the videos were downloaded. He then obtained a subpoena that was served on the internet service provider for the identity and address of the owner[4] of the IP address on May 3, 2007, between 11:00 am and 2:00 pm.[5] The service provider responded on May 23, 2007, identifying the name and address of Charles Borowy.

On July 11, 2007, Special Agent Jeff Cotner prepared and filed an affidavit for a search warrant based in large part on Agent Mitchell's investigation. (Mot. to Suppress (#20) at 2.) The warrant was executed on July 12, 2007, and numerous items were seized during the search including

---

[3]IP addresses are uniquely assigned to each computer on the internet.

[4]The owner of an IP address may not be the same as the user. In addition, a user need not be present at his computer during the file-sharing process.

[5]IP addresses are often reassigned periodically, but service providers are usually capable of identifying which IP address is assigned to which computer at a certain time.

Borowy's laptop computer, CDs, and floppy disks. (*Id.*)

II. Discussion

The threshold issue the court must decide is whether Agent Mitchell's conduct constituted a search within the meaning of the Fourth Amendment. *See* U.S. Const. amend. IV. A criminal defendant may invoke the protections of the Fourth Amendment–including the exclusionary rule–"only if he can show that he had a legitimate expectation of privacy in the place searched or the item seized." *United States v. Ziegler*, 474 F.3d 1184, 1189 (9th Cir. 2007) (emphasis omitted) (*quoting Smith v. Maryland*, 442 U.S. 735, 740 (1979)). A defendant can establish this expectation by showing (1) a subjective expectation of privacy and (2) an objectively reasonable expectation of privacy. *United States v. Shryock*, 342 F.3d 948, 978 (9th Cir. 2003).

In this case, Borowy did not have a legitimate expectation of privacy in files he made available to others using P2P software. First, it is not apparent that Borowy had a subjective expectation of privacy in these files. While the sharing of apparent child pornography may create an inference that Borowy expected privacy in his files, Borowy does not contend that he had such an expectation. Nor do the circumstances of Borowy's file-sharing suggest a subjective expectation of privacy. *See United States v. Sandoval*, 200 F.3d 659, 660 (9th Cir. 2000). For example, any Limewire user could search for files currently being shared on the P2P network and locate Borowy's files. Making these files available to any Limewire user is consistent with a lack of an expectation of privacy. Therefore, Borowy has failed to carry his burden to prove he had a subjective expectation of privacy. *United States v. Caymen*, 404 F.3d 1196, 1199 (9th Cir. 2005).

Second, even assuming Borowy had a subjective expectation of privacy, his expectation was objectively unreasonable. The Tenth Circuit held in a similar case that access to peer-to-peer software, "to the extent such access could expose . . . information to outsiders, . . . vitiates any expectation of privacy [the defendant] might have had in his computer and its contents." *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008).

Furthermore, in *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007), the Ninth Circuit considered the objective reasonableness of privacy expectations an employee may have in files stored on his work computer. The court first noted that employees retain at least some expectation of privacy in their offices. *Ziegler*, 474 F.3d at 1190. In considering the circumstances of files seized from Ziegler's computer, the court further observed that "[h]is office was not shared by co-workers, and kept locked." *Id*. These circumstances led the court to conclude that Zeigler's well-established subjective expectation of privacy was reasonable. *Id*.

Here, the type of exclusive use relied upon by the *Ziegler* court in finding an objectively reasonable expectation of privacy is absent. *See also Schowengerdt v. United States*, 944 F.2d 483, 487 (9th Cir. 1991) ("Schowengerdt would enjoy a reasonable expectation of privacy in areas given over to his exclusive use . . . ."). Borowy made available his personal files to other Limewire users, rendering his use of shared files nonexclusive.

The relative anonymity and volume of users who might gain access to Borowy's files using Limewire imply less exclusivity than a shared office space. *See Mancusi v. DeForte*, 392 U.S. 364, 369 (1968). In *Mancusi*, the Supreme Court found an objectively reasonable expectation of privacy on the part of one office-mate because he could expect that he would not be disturbed except by business or personal guests and that his files would not be taken except with his permission. *Mancusi*, 392 U.S. at 369. Here, in contrast, any Limewire user–such as a federal agent–could survey and download the files Borowy shared through Limewire. In addition, Borowy did not restrict access to his shared files by some mechanism (such as a password) that granted access only with his permission. Thus, there is no evidence to suggest any expectation of privacy in Borowy's shared files was reasonable. *See Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *see also Lewis v. United States*, 385 U.S. 206, 210 (1966) (holding that representations made to an undercover agent were admissible where the agent exercised no

governmental power to intrude upon the defendant's privacy); *cf. Smith v. Maryland*, 442 U.S. 735, 744 (1979) (holding that where a defendant voluntarily conveys information to a third party, the defendant assumes the risk that the third party will turn the information over to the police). Therefore, Agent Mitchell's conduct was not a search within the meaning of the Fourth Amendment.

Both Borowy and the government discuss the "plain view" doctrine with respect to Agent Mitchell's conduct. This is appropriate since the "legitimate expectation of privacy" test is supported by the reasoning underlying the plain view doctrine. *Illinois v. Andreas*, 463 U.S. 765, 771 (1983). "The plain view doctrine authorizes seizure of illegal or evidentiary items visible to a police officer whose access to the items has some prior Fourth Amendment justification and who has probable cause to suspect that the item is connected with criminal activity." *Id*. The plain view doctrine is grounded "on the proposition that once police are lawfully in a position to observe an item first-hand, its owner's privacy interest in that item is lost." *Id*. In this sense, the plain view doctrine is just an extension of the original justification for an intrusion. *Horton v. California*, 496 U.S. 128, 136 (1990). Borowy consequently argues that Agent Mitchell did not have a prior Fourth Amendment justification to access Borowy's files, that Agent Mitchell's conduct in viewing the content of these files went beyond a plain view seizure, and that Agent Mitchell had no probable cause to view the files. Alternatively, Borowy contends that material misrepresentations in the affidavit supporting the search warrant undermine the search warrant.

First, Borowy argues that Agent Mitchell's "entrance" into Borowy's computer was unlawful because Agent Mitchell did not have a prior Fourth Amendment justification granting him access to Borowy's files. However, since Borowy had no legitimate expectation of privacy in his shared files, Borowy did not suffer a Fourth Amendment intrusion when Agent Mitchell accessed these files. Moreover, there is no indication that Agent Mitchell's actions differed from those which could be taken by any member of the public. *Cf. Lo-Ji Sales Inc. v. New York*, 442 U.S. 319, 329

(1979). Therefore, since Agent Mitchell's conduct did not constitute a search, Agent Mitchell did not violate the Fourth Amendment by accessing Borowy's computer files through Limewire. *See id.*; *see also Payton v. New York*, 445 U.S. 573, 586-87 (1980) (holding that contraband found in a public place may be seized by the police without a warrant).

Second, Borowy argues Agent Mitchell manipulated the files beyond what is allowable by the plain view doctrine by downloading and viewing them. However, assuming downloading and viewing the files was a seizure under the Fourth Amendment, Agent Mitchell had probable cause under the plain view doctrine to seize the files based on their names. Borowy's files were named in such a way as to suggest the files contained child pornography. For example, one such video was entitled CPTVG 13 bond 10–11-12yo Childlover little collection video39girl.[6] (Mot. to Suppress (#20), Cotner Aff., Ex. A ¶ 32.) These names create a fair probability that the files contained child pornography. *See Illinois v. Gates*, 462 U.S. 213, 232 (1983). Therefore, to the extent downloading and viewing Borowy's files constituted a seizure, Agent Mitchell had probable cause to seize the files.

In addition, viewing the files was not a search within the meaning of the Fourth Amendment, because Borowy did not have a legitimate expectation of privacy in their contents. Because Borowy was sharing the files using a P2P file-sharing program, he had neither a subjective nor a reasonable expectation of privacy. Moreover, even if viewing the files was a search, the filenames provided justification for a warrantless viewing of their content under the "single-purpose container" exception to the warrant requirement. The single-purpose container exception is "little more than another variation of the 'plain view' exception, since if the distinctive configuration of a container proclaims its contents, the contents cannot fairly be said to have been removed from a

[6]Two of the filenames were not explicitly suggestive of child pornography: "New!! PTHC Sec lessons-jerking & facial– show this training video" and "fdsa 5-3yo girl." (Mot. to Suppress (#20), Cotner Aff., Ex. A ¶ 32.) However, the five remaining suggestive filenames constitute sufficient probable cause for a seizure and search of these files.

searching officer's view." *Robbins v. California*, 453 U.S. 420, 427 (1981) (plurality opinion); *see also United States v. Gust*, 405 F.3d 797, 800 (9th Cir. 2005) (recognizing the continued applicability of the single-purpose container exception). Here, the filenames are explicit enough that "the container is such that its contents may be said to be in plain view." *Gust*, 405 F.3d at 800. Therefore, Agent Mitchell's viewing of the files' content did not require a warrant.

Additionally, probable cause to issue the search warrant existed even without reference to the content of the videos. *See Gates*, 462 U.S. at 232 ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place."). The filenames themselves, apart from their content, gave the magistrate probable cause to issue a search warrant.

Finally, Borowy argues material misrepresentations in the affidavit in support of the search warrant undermine probable cause for the issuance of the search warrant. To challenge a search warrant on the basis of misrepresentation, a defendant must make a substantial preliminary showing that the affidavits in support of the warrant contained intentionally or recklessly false material statements. *Franks v. Delaware*, 438 U.S. 154, 171 (1978). If this preliminary showing is made, the court must then hold a hearing to examine the affidavits. *Id*. In this hearing, the court must determine if, excluding the misrepresentations, probable cause would exist on the basis of the remaining information. *Id*. If, without the exclusions, probable cause is lacking, the search warrant is defective and the evidence seized thereunder is excluded. *Id*.

Borowy argues that appearance of the videos' descriptions next to their filenames in the affidavit created a false implication that the descriptions were part of the filenames. (Mot. to Suppress (#20) at 2.) As an initial matter, Borowy's argument is without merit because the affidavit makes sufficiently clear that the descriptions are not part of the filenames by identifying the filenames with the handle "Filename:" and the descriptions with the handle "Description:". (Mot. to

Suppress (#20), Cotner Aff., Ex. A ¶ 32.) Thus, Borowy has failed to make a substantial preliminary showing of misrepresentations included in the affidavit, and a *Franks* hearing is not warranted. Moreover, including descriptions of the files' contents in the affidavit was proper because the contents were not revealed pursuant to a search, and, even if it was a search, the contents were lawfully revealed pursuant to the single-purpose container exception to the warrant requirement. Finally, as stated previously, the affidavit sufficiently set forth probable cause for a search warrant based solely on the filenames.

IT IS THEREFORE ORDERED that Borowy's Motion to Suppress (#20) is DENIED.

IT IS SO ORDERED.

DATED this 28th day of August 2008.

LARRY R. HICKS
UNITED STATES DISTRICT JUDGE